UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/701,154 | 11/03/2003 | Massimiliano Antonio Poletto | RIV-0510 | 5561 |

87555 7590 07/17/2009

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

| EXAMINER | |
|---|---|
| MEHRMANESH, ELMIRA | |
| **ART UNIT** | **PAPER NUMBER** |
| 2113 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 07/17/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 10/701,154
Filing Date: November 03, 2003
Appellant(s): POLETTO ET AL.

Denis G. Maloney
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed January 22, 2009 appealing from the Office action mailed August 6, 2008.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the response to the notification of non-compliant appeal brief filed April 7, 2009 is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

Ontiveros et al. (U.S. PGPub 20020107953) published on August 8, 2002.

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5, 7-16, 18-22, and 28-32 are rejected under 35 U.S.C. 102 (e) as being anticipated by Ontiveros et al. (U.S. PGPub 20020107953).

As per claim 1, Ontiveros discloses a system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network (paragraph [0024])

an aggregator device that receives the connection information from the plurality of collector devices (paragraph [0037]), and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node (paragraph [0040]), with the aggregator device further comprising:

a process executed on the aggregator device to detect anomalies in connection patterns (paragraphs [0008] and [0024])

a process executed on the aggregator device to aggregate detected anomalies into the network events (paragraph [0026], Anomaly Detection System) with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies (paragraphs [0003] and [0024]).

As per claim 2, Ontiveros discloses the aggregator determines at least in part from the connection patterns derived from the connection table occurrences of network events (paragraph [0008], Intrusion Detection System).

As per claim 3, Ontiveros discloses the aggregator further comprises: a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator (paragraph [0037]).

As per claim 5, Ontiveros discloses the collector devices have a passive link to devices in the network (Fig. 1).

As per claim 7, Ontiveros discloses the anomalies include unauthorized access and worm propagation (paragraphs [0003] and [0024]).

As per claims 8, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address (paragraphs [0040] and [0044]).

As per claim 9, Ontiveros discloses the connection table includes a plurality of records that are indexed by destination address (paragraphs [0040] and [0045]).

As per claim 10, Ontiveros discloses the connection table includes a plurality of records that are indexed by time (paragraphs [0040] and [0049]).

As per claim 11, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (paragraphs [0040]-[0049]).

As per claim 12, Ontiveros discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (paragraph [0042]).

As per claim 13, Ontiveros discloses the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (paragraphs [0042]-[0049]).

As per claim 14, Ontiveros discloses a method, comprises:

sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices (paragraph [0024])

producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic from the node (paragraph [0040]), with the connection table including a plurality of entries that are indexed by source address (paragraphs [0040] and [0044]).

As per claim 15, Ontiveros discloses collecting statistical information in the collector devices to send to the aggregator device (paragraph [0024]).

As per claim 16, Ontiveros discloses determining from the connection information and the statistical information occurrences of network anomalies (paragraphs [0008] and [0024]); and aggregating anomalies into network events (paragraph [0026]) that indicate potential network intrusions (paragraph [0008], Intrusion Detection System) and communicating occurrences of network events to an operator (paragraph [0057], system administrator).

As per claim 18, Ontiveros discloses the connection table includes a plurality of records that are indexed by destination address (paragraphs [0042] and [0045]).

As per claim 19, Ontiveros discloses the connection table includes a plurality of records that are indexed by time (paragraphs [0040] and [0049]).

As per claim 20, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (paragraphs [0040]-[0049]).

As per claim 21, Ontiveros discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (paragraph [0042]).

As per claim 22, Ontiveros discloses the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (paragraphs [0042]-[0049]).

As per claim 28, Ontiveros discloses a storage medium storing a computer program product, the computer program product comprising instructions for causing a computer to:

collect connection information to identify host connection pairs from packets that are sent between nodes on a network and produce a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node (paragraph [0037]);

detect anomalies in connection patterns (paragraphs [0008] and [0024]);

and aggregate detected anomalies into the network events (paragraph [0026], Anomaly Detection System) with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies (paragraphs [0003] and [0024]).

As per claim 29, Ontiveros discloses instructions to determine at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions (paragraph [0008], Intrusion Detection System).

As per claim 30, Ontiveros discloses instructions to collect statistical information on packets that are sent between nodes on a network (paragraph [0037]).

As per claim 31, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (paragraphs [0040]-[0049]).

As per claim 32, Ontiveros discloses the connection table includes a plurality of connection sub-tables to track data at different time scales, the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table

with each sub-table holding the sum of records received from all collectors during respective units of time (paragraphs [0040]-[0049]).

**(10) Response to Argument**

As per claims 1, 14 and 28, in response to applicant's arguments that Ontiveros fails to disclose “a connection table that maps each node of a network to a record that stores information about packet traffic to or from the node”, the Examiner respectfully disagrees and would like to point out to paragraph [0038] wherein Ontiveros discloses a table to count the number of times a particular pair of source and destination IP addresses is detected. Entries are stored using a hash table, keyed by the source and destination addresses.

Note paragraphs [0041] through [0049] wherein Ontiveros further discloses cataloging packets by sorting data with various keys such as Source Address and Destination Address.

It is apparent that a table storing information about network packet traffic between a source and a destination as discloses by Ontiveros reads on the claimed limitation of “a connection table that maps each node of a network to a record that stores information about packet traffic to or from the node”, as recited in the above claims.

Applicant further argues that Ontiveros fails to disclose a process executed on the aggregator device to detect anomalies in connection patterns. The Examiner respectfully disagrees and would like to point out to paragraphs [0043] through [0050],

wherein Ontiveros discloses sorting data by Source Address, Destination Address, and Source Destination Address…Using these primary data types, the present invention can sort data type attacks and protocol types to identify new patterns, as well as catalog usage patterns and usage profiles. Using the keys, **a hash table can be created to monitor for and determine data attack types** depending upon the particular security needs of the network. Monitoring source and destination address (i.e. node to node connections) and identifying certain patterns reads on the claimed limitation.

Applicant further argues that Ontiveros fails to disclose a process executed on the aggregator device to aggregate detected anomalies into the network events. The Examiner respectfully disagrees and would like to point out to paragraph [0024] wherein Ontiveros discloses monitoring and detecting traffic with patterns that are in contrast to normal traffic patterns. Thus detecting events associated with attacks.

In response to the Appellant's arguments with respect to claims 2, 16 and 29 that Ontiveros fails to disclose "…wherein the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.", the Examiner respectfully disagrees and would like to point out to paragraph [0008] wherein Ontiveros discloses an intrusion detection system (IDS). Further note paragraph [0024] wherein Ontiveros discloses "…detects and denies data traffic with patterns that are in contrast to normal traffic patterns (i.e., exceed user defined configurable parameters), thereby preventing hacking attacks on networks. Depending upon the security requirements of the network, the present invention may be configured to detect different levels of attacks." Therefore,

the prior art teaches the invention as claimed and the above claims do not distinguish over the prior art as applied.

In response to the Appellant's arguments with respect to claims 8, 9, 18, and 19 that "Ontiveros does not describe the connection table and specifically the features of that the connection table includes a plurality of records that are indexed by source address", the Examiner respectfully disagrees and would like to point out to paragraphs [0043] through [0047] wherein Ontiveros discloses cataloging packets by sorting data with various keys such as Source Address and Destination Address.

It is apparent that a table storing information about network packet traffic between a source and a destination as discloses by Ontiveros reads on the claimed limitation of "the connection table and specifically the features of that the connection table includes a plurality of records that are indexed by source address", as recited in the above claims. Therefore, the prior art teaches the invention as claimed and the above claims do not distinguish over the prior art as applied.

In response to the Appellant's arguments with respect to claims 10-13, 20-22, 31 and 32 that "Ontiveros does not describe any structure that stores records according to the sampling time. In contrast, claim 10 requires that the records are indexed by time.", the Examiner respectfully disagrees and would like to point out to paragraphs [0040] through [0049] wherein Ontiveros discloses cataloging packets by sorting data with various keys such as time/date stamp.

It is apparent that a table storing information about network packet traffic between a source and a destination as discloses by Ontiveros reads on the claimed limitation of “the connection table includes a plurality of records that are indexed by time”, as recited in the above claims. Therefore, the prior art teaches the invention as claimed and the above claims do not distinguish over the prior art as applied.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner’s answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Elmira Mehrmanesh

/Robert W. Beausoliel, Jr./
Supervisory Patent Examiner, Art Unit 2113

Conferees:

/RB/
Robert Beausoliel
Supervisory Patent Examiner, Art Unit 2113

Mark Rinehart
/M. R./
Supervisory Patent Examiner, Art Unit 2111